Raul Benitez Netto

Threat Analyst / IR / SOC Tier 3

Asunción, Paraguay (UTC-4)
(+595) 975603978
raulbeni@gmail.com
https://www.linkedin.com/in/rauliss/
https://about.me/rauliss

A **threat analyst** with 7+ years performing incident response and analysis of compromised systems and networks. My experiences working **Linux** and cloud environments is high. I've participated in the research team of many incidents and some of them categorized as APT (Advanced Persistent Threat). Also, I have experience being a full stack developer with 12+ in the software industries working with technology like **Python, Ruby, Java and PH**P. Solid knowledge of frameworks and libraries in different development stacks such as **ReactJS, Electron** (making hybrid applications), jQuery in the frontend, and also **Ruby on Rails, Django and CakePHP** in the backend. I have **leadership skills** and experience leading a threat analysts team in the national CERT-PY. My vision as software developer and threat analyst make me a versatile engineer which can be an important piece in a security area of a tech company. I envision my future career in an international tech company as a tech lead being part of its **SOC team** or part of the **DevOps** team being a **security enginee**r.

EXPERIENCE

Beacon Lab - Cybolt

Incident Response Specialist *— September 2023 - Present*

- Being part of the analyst team in more than seven (7) cyber incidents categorized as Critical. These attacks were performed by bands like Akira, Trigona, Mallox and others
- Design and work of more than 4 cyberdrills and incident response tabletop. Being part of Red and blue strategies and ejecution.
- Working to establish the CSIRT, selecting tools, technology.
- Working closely to plan, design and execute cyber exercise as a service for several Cybolt's clients.
- Working closely with the Checkmarx SAST/DAST Tool and performing code review and pentesting in web development projects written in PHP, Python, Ruby and CGI

Tech Stack: Python, Elastic Search, Kibana, Logstash, Linux, Linux Shell/Bash, Window Logging System, MISP, Promox PVE, pfsense, Docker, Swarm, Cisco Umbrella.
Skill: Leadership, Teamworking, Problem-Solving, Analytical Thinking

CERT-PY - Ministerio de Tecnologia de la Información y Comunicación

Incident Management Operational Supervisor (Threat Analyst Lead tier 1) *— November 2019 - September 2023*

- I've established the first CERT-PY incident response procedures manual which defines the guide and baselines (Incident taxonomy, definition of criticalities at government and private sector level, basic training manual for on-boarding, definition of rejection and escalation procedures and others) for team workflow.
- I actively participated in the evaluation of the design of the Governamental SOC proposal. I focused on the evaluation of technology and training proposals, in addition to the design of the organizational chart and the distribution of functions of the Governamental SOC.
- During my first year I was able to resolve about x17 times more incidents than previous years. From 80 to ~1400 incidents.
- I managed to mark incident response times of 24 hours on average per month and resolution time of 72 hours on average. Previously they were 30 and 90 days respectively. These achieved times became standard within the team.
- I was able to develop 3 report processing automation tools. All made in Python. All of them integrated different services and communication channels with our Request Tracker - Incident Response (RTir) ticketing system.
- I've implemented a set of tools to process around 30k IoC feeds received per day from different sources.
- I've performed more than 100 incidents related to compromised web servers.
- I have led incident analysis in more than 40 incidents qualified as high criticality and in an APT attack (with a detection delay of approximately 30 days).
- I created more than 150 security warnings, regarding vulnerabilities affecting technology being used in the country or malicious campaigns being performed inside paraguayan territory .

Tech Stack: Python, Elastic Search, Kibana, Logstash, Linux, Linux Shell/Bash, Window Logging System, IntelMQ, MISP, Promox PVE, pfsense, Docker, Swarm, pihole, AWS Security sets, Cisco Umbrella.
Skill: Leadership, Teamworking, Problem-Solving, Analytical Thinking

Freelancer Forensic Analyst — *November, 2020 - Present*

- I have helped the prosecutor of the city of Encarnación - Paraguay to clarify a murder case.
- I worked in more than 7 criminal, civil and commercial cases related to data extraction from various devices and system

audits.

Tech Stack: python, DVR Extract, WhatsApp, ExifTool, Autopsy, SIFT Workstation
Skill: Analytical Thinking

Integradevs Software Solutions, Web Developer

ClearForms / ClearGov — *September, 2022 - May, 2023*

- I have implemented a login system with Auth0 for integrating a variety of ClearGov's projects with an unique SSO. MFA logic was included too. Actually it is being used by more than 4k users with admin roles. This system is helping with the integration of various projects of the company and adding a security layer for the admin users.

Tech Stack: React.JS, Ruby on Rails, Docker, Heroku, Auth0
Skill: Teamworking, Problem-Solving

SmartLunches — *January, 2012 - September, 2015*

- I have created a web system to order food for kids by their parents. It had a partnership with Schools in Boston where the meals were delivered. The system allows you to choose the day and the food for your kid by hand or it can be automatically selected by a system according to likes. It helped more than 5k users at that time.
- Previously they used a third-party web app with no control of the UI or any workflow in the system. The admin dashboard provided a complex UI for creating meals. For that, I had to create a script in PHP to read an Excel spreadsheet with meals data and create them in the web system..

Tech Stack: jQuery, Ruby on Rails, Heroku, Postgres SQL
Skill: Teamworking, Problem-Solving

DarkWaves, Pentester Consultant Junior — *April, 2022 - July, 2022*

- Performed analysis of 2 projects (web and mobile)

Tech Stack: Burp Suite, OWASP Suite, Nmap, Mobile-Security-Framework-MobSF, Hexway Hive
Skill: Problem-Solving, Analytical Thinking

MMF System, Software Developer — *September, 2018 - December, 2021*

- I helped in the construction of one integration between a fax page (TIFF) processor with a SOAP Java System with Machine Learning and OCR detection. Reducing the tasks presion to human analysts by ~56% for processing patients' medical records for hospitals around the USA. Before the patients' medical records were sent via fax directly to a human operators team and were manually processed. It means, the records were read, identified, classified and stored in a Java Web Application.
- We developed a Django web app to migrate the old system written in Java. We were not able to release it.

Tech Stack: Python, Matplotlib, Pandas, OCR, Django, Vagrant, GitLab, SQL.
Skill: Teamworking, Problem-Solving

SingleCase.cz, Web Developer — *October, 2017 - December, 2018*

- Contributed for building a web software solution for lawyers, refactoring and improving the business logic into the legacy codebase.
- Created a hybrid app for macOS and windows systems with Electron.

Tech Stack: ElectronJS, NodeJS, PHP, CakePHP, Docker.
Skill: Teamworking, Problem-Solving

Stratosphere Lab - +Faculty of Electrical Engineering, Czech Technical University

Junior Researcher - Stratosphere Lab — *May, 2016 - August, 2018*

- Created a Machine Learning Model to measure the WHOIS Similarity Distance https://github.com/stratosphereips/whois-similarity-distance of two given domains with a 95% TP rate.

Tech Stack: Python, Matplotlib, Pandas, Machine Learning Models

Web Developer - Stratosphere Lab — *May, 2016 - August, 2018*

- Created a web application for providing threat analysts a fast interface and analysis tools to speed up their research https://www.stratosphereips.org/manati. It was presented in 3 conferences and it was validated by 1 threat analyst team.

Tech Stack: Python, Django, jQuery
Skill: Problem-Solving, Analytical Thinking

SKILLS

Programming Languages: Advanced: Ruby, Python, JavaScript; Intermediate: PHP; Basic: Java.
Frameworks Tools: Advanced: Django, Ruby on Rails; Intermediate: CakePHP, Electron, ReactJS; Basic: JSP.
Data Base: Intermediate: Postgres, MySQL, SQLite; Basic: Elasticsearch.
Tools: Advanced: Linux shell, Docker, Heroku, Virtual Box; Intermediate: Vagrant, Heroku, Digital Ocean, AWS, Burp Suite, GitHub, Gitlab; Basic: Terraform, Ansible, Kubernetes, OwaspZap.

Agile: Kanban, Scrum,
Languages: Advanced: English; Native: Spanish.

EDUCATION

Czech Technical University– Prague. *Master of Science, Computer Security, September 2018*
National University of Itapua – Encarnación. Computer Engineering, December 2014

CERTIFICATIONS

Certified SOC Analyst v1 – EC-Council. 2022.
Certified Incident Handler v3 – EC-Council. 2024.

Courses

National University of Defense – Washington DC, Policy Development Course - CYBER in the Perry Center, *July 2023*
Invictus Incident Response *- Las Vegas, DEFCON TRAINING - Incident Response in the Microsoft Cloud, August 2024*